

## UNITED STATES DISTRICT COURT

for the  
District of New Mexico**FILED**  
UNITED STATES DISTRICT COURT  
LAS CRUCES, NEW MEXICO

JUN 05 2024

MITCHELL R. ELFERS  
CLERK OF COURTIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)10335 Cedar Springs Place NW, Albuquerque, New  
Mexico

Case No.

24-1085MR

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, attached hereto and incorporated herein.

located in the \_\_\_\_\_ District of \_\_\_\_\_ New Mexico \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, attached hereto and incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

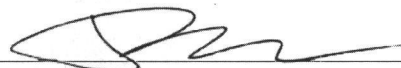
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 875(c)	Threats in Interstate Communications

The application is based on these facts:

See attached affidavit in support of an application for a search warrant

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



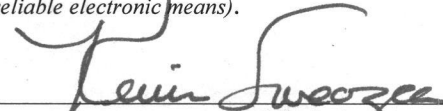
Applicant's signature

Jacob vanBrandwijk, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by \_\_\_\_\_ (specify reliable electronic means).

Date: 06/05/2024



Judge's signature

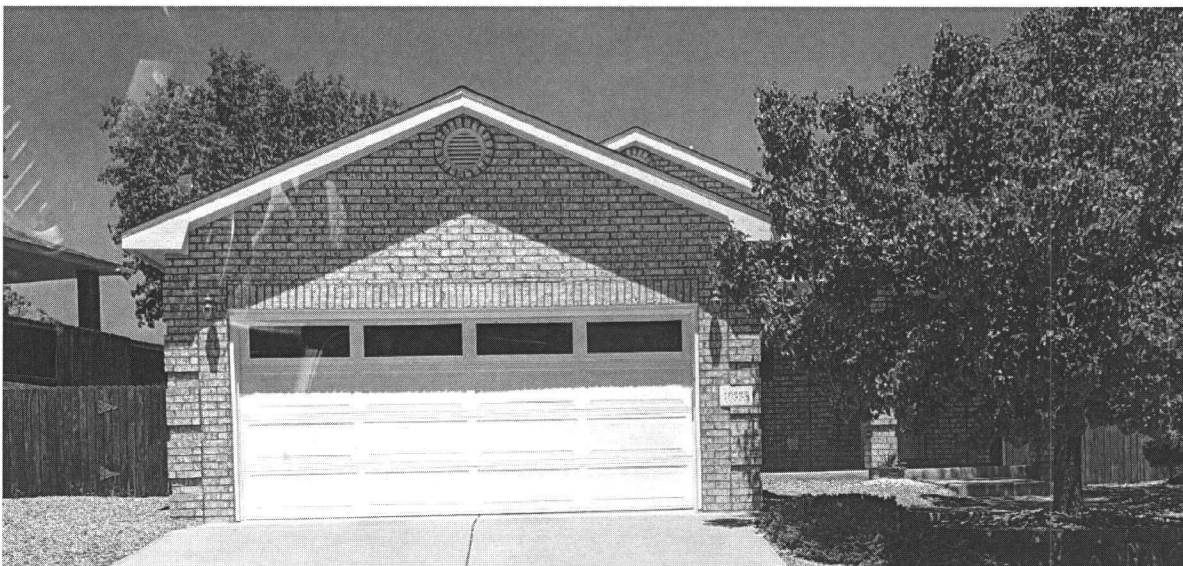
City and state: Las Cruces, New Mexico

Kevin Swearingen United States Magistrate Judge  
 Printed name and title

**ATTACHMENT A**

***Property to be searched***

10335 Cedar Springs Place NW, Albuquerque, New Mexico, described as a residence with brick façade, and attached garage bearing a light colored placard marked 10335 and pictured below.



ATTACHMENT B

*Property to be seized*

1. All records relating to violations of 18 U.S.C. § 875, those violations involving Olsi Vrapı, including records relating to victims TBE or similar organizations, or others relevant to this investigation and pertaining to:
  - a. Any and all records reflecting threats or extortion sent in interstate communications
2. Any and all electronic devices that may have been used as a means to commit the violations described above, including:
  - a. Computers and electronic storage devices
  - b. Routers, modems, and network equipment
  - c. Cellular telephone devices
3. Any and all records of telecommunications services, including telephone billing records and internet subscriber records.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.



IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF:  
10335 Cedar Springs Place NW,  
Albuquerque, New Mexico

Case No.

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Jacob vanBrandwijk, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 10335 Cedar Springs Place NW, Albuquerque, New Mexico, herein after THE PREMISES, further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since March, 2017. While employed by the FBI, I have investigated federal criminal violations related to high technology or cyber crime. I have gained experience through training and everyday work relating to conducting these types of investigations. Prior to becoming a Special Agent of the FBI, I earned a Bachelor's degree in Computer Science and Master's degree in Information Assurance, and was employed in the field of information security full time for thirteen years. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. § 875, and I am authorized by the Attorney General to request a search warrant.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The

information contained in this affidavit is personally known to me based on my training and experience, was gathered or revealed to me personally during the course of this investigation, or was gathered or revealed to other sworn law enforcement officers during the course of this investigation and subsequently communicated to me.

4. Based on the information set forth herein, there is probable cause to believe that violations of 18 U.S.C. § 875(c) (Threats in Interstate Communications) were committed, and that evidence of these violations may be found within THE PREMISES.

#### PROBABLE CAUSE

##### *Terms*

##### Internet Service Providers

5. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses with access to the Internet through access accounts. Subscribers obtain an account by registering with ISPs. During the registration process, ISPs ask subscribers to provide basic personal information. Additionally, ISPs are likely to maintain records and information concerning subscribers and their use of the ISP’s services, such as account use and access information and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

##### IP Addresses

6. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses are provided by ISPs and are used to identify a computer on a network. IP addresses can be “dynamic,” meaning that the ISP assigns a different

unique number to a computer every time it accesses the Internet. IP addresses might also be “static” if an ISP assigns a user’s computer a particular IP address, which is used each time the computer accesses the Internet. In my training and experience, ISPs commonly maintain records of which subscriber used an IP address, and the period of time for which that subscriber used that IP address. As such, the identification of an IP address that used an internet service, such as Google Gmail, at a given time can lead to the identification of the individual subscriber.

### ***Background***

7. On June 4, 2024, Special Agent Roberts of the FBI’s Albuquerque Division, Las Cruces Residence Agency received information from the Las Cruces Police Department that a local religious organization in Las Cruces, NM, hereafter referred to as TBE, had received a threatening communication to their email address. On that same date, I viewed a copy of this email, and observed that the email stated, approximately and in part “Gonna fucking kill of you!” and “Gonna drive down there and shoot and kill as many people and fucking bomb you [...]” I have omitted portions of this email which may tend to identify the organization threatened, and attest that the omitted portions do not contain information which changes the meaning of the included portions. I also noted that this email came from the email address [olsivrap@gmail.com](mailto:olsivrap@gmail.com).

### ***Acts Under Investigation***

8. On the same date, I made contact with representatives of TBE, hereafter KN and EL, and confirmed that they had received the email described above. Both KN and EL stated that the content of the message had put them in fear. KN stated that she managed the email account which had received the message, and that this account was publicly posted by the organization and was regularly used to conduct the business of the organization.

9. I searched FBI databases for the term olsivrap and identified two additional threats which I believe to be related. The first was sent to a similar organization in Santa Fe, NM by the email address olsivrap3456@proton.me in late May of 2024. The second was sent from the tutamail.com address described above, again to a similar organization, in Denver, CO on or about June 4, 2024.

10. On June 5, 2024, I requested that Meta Platforms Inc. voluntarily disclose, pursuant 18 U.S.C. § 2702, subscriber information for any accounts registered with either of the email addresses described above. Meta Platforms Inc. disclosed three accounts, which were registered using variations of the name Olsi Vrap, and included the IP addresses used for registering these accounts: 174.28.171.23 for a Facebook account associated with olsivrap3456@proton.me, 174.28.56.191 for an Instagram account associated with olsivrap3456@proton.me, and 174.28.68.156 for a Facebook account associated with olsivrap@tutamail.com.

11. In North America, IP addresses are assigned to ISPs by the organization American Registry of Internet Numbers (ARIN). On the same date, I requested information from ARIN regarding the ISP responsible for the IP addresses provided by Meta Platforms Inc. ARIN identified that all three IP addresses were all managed by the ISP CenturyLink. Based on open source research, I learned that CenturyLink is now referred to as Lumen Technologies.

12. I requested that Lumen Technologies voluntarily disclose, pursuant 18 U.S.C. § 2702, subscriber information for any accounts which used the IP addresses provided by Meta Platforms Inc. at the times identified by Meta Platforms Inc. Lumen technologies was unable to identify a subscriber associated with the IP address 174.28.171.23 because the registration time



provided was too far in the past. However, both of the remaining IP addresses were registered to Farrar Rental House, 10335 Cedar Springs Place NW, Albuquerque, NM, THE PREMISES.

13. I know, based on my training and experience, that tutanota.com is an email service provider headquartered in Germany. I observed the headers on the email sent to TBE, which contain meta information about from where the email was sent and the path it traveled on the internet, and learned that this particular email was sent from the IP address 81.3.6.162. Réseaux IP Européens Network Coordination Centre (RIPE) is the European equivalent of ARIN. On the same date, I requested information from RIPE regarding the ISP responsible for the 81.3.6.162. RIPE provided information that this IP was administered by Tutao GmbH, the company which operates tutamail.com. I therefore believe that whomever sent the email to TBE did so by using Tutao's email servers in Germany, and that thus this communication, in travelling to TBE in Las Cruces, necessarily traveled in interstate and foreign commerce. Because this communication contained a threat to kill another person, I believe that whomever sent this message did so in violation of 18 U.S.C. § 875(c).

#### ***THE PREMISES***

14. Based on the foregoing, I believe that an electronic device or devices present in THE PREMISES was used to access social media accounts controlled by the same person or persons who communicated a threat to TBE in foreign commerce. I further believe that by reviewing the contents of these electronic devices, the FBI may learn the identity of this person or persons. I therefore believe that evidence of violations of 18 U.S.C. § 875(c) may be found at 10335 Cedar Springs Place NW, Albuquerque, NM, THE PREMISES.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

15. As described above and in Attachment B, this application seeks permission to search for records that might be found on THE PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

16. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.  
  
Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

17. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in THE PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that



log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to perform a denial of service attack, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a

computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

18. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from THE PREMISES, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on THE PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

20. Because several people may share THE PREMISES as a residence, it is possible that THE PREMISES will contain computers and storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those



computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

21. Based on the aforementioned information and investigation, I submit that probable cause exists to search THE PREMISES, as more particularly described in Attachment A and to seize the items described in Attachment B.

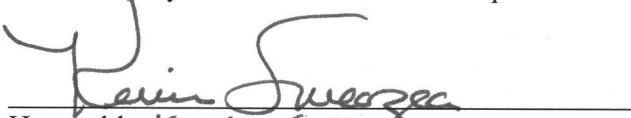
**Reviewed by AUSA Christopher McNair**

Respectfully submitted,



Jacob vanBrandwijk  
Special Agent  
Federal Bureau of Investigation

Electronically submitted to me and telephone sworn on June 5, 2024



Honorable *Kevin Swearing*  
UNITED STATES MAGISTRATE JUDGE